Attorney Docket No.: 42P17259 Patent Application

UNITED STATES PATENT APPLICATION
FOR

SESSION KEY EXCHANGE

INVENTORS:

WILLARD M. WISEMAN,
a citizen of the United States

DAVID W. GRAWROCK,
a citizen of the United States

ERNIE BRICKELL,
a citizen of the United States

MATTHEW D. WOOD,
a citizen of the United States

JOSEPH F. CIHULA,
a citizen of the United States

PREPARED BY:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030
(303) 740-1980

EXPRESS MAIL CERTIFICATE OF MAILING
"Express Mail" Mailing No. EV US 331619551 US

I hereby certify that I am causing the above-referenced correspondence to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated below and that this paper or fee has been addressed to the Commissioner for Patents, Patent Application, P.O. Box 1450, Alexandria, VA 22313.

Date of Deposit: December 30, 2003
Name of Person Mailing Correspondence: Krista Mathieson

Krista Mathieson
Signature

December 30, 2003
Date

SESSION KEY EXCHANGE

FIELD

[0001] An embodiment of the invention relates to secure computer operations in general, and more specifically to session key exchange.

BACKGROUND

[0002] In network operations, various methods have been used to provide security in operations. The increasingly large number of connected users results in a high degree of risk if secure operations are not maintained. For this reason, it is extremely important to provide a system that will allow the establishment of trust between various parties.

[0003] If a first agent (a client) desires a service from a second agent (a service provider), the second agent may require proof of the authority and authenticity of the first agent before providing the service. The second agent requires assurance that the first agent will not misappropriate information, attack the system, or otherwise cause damage. When such assurance is obtained, a session key may be issued, the session key providing confidentiality, integrity, or both to the services requested and rendered.

[0004] However, providing assurance of secure operations can impose a large amount of overhead on a system. Further, conventional processes may not provide sufficient security. Providing assurance of the use of a service on a particular platform or platforms may not provide assurance of the particular environment in which the service is applied.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The invention may be best understood by referring to the following description and accompanying drawings that are used to illustrate embodiments of the invention. In the drawings:

[0006] **Figure 1** illustrates an embodiment of network operations;

[0007] **Figure 2** illustrates an embodiment of a session key exchange utilizing a trusted third party;

[0008] **Figure 3** illustrates an embodiment of a session key exchange utilizing a protocol to establish trust without a trusted third party;

[0009] **Figure 4** illustrates an embodiment of a session key exchange without identification of the exact configuration of the client; and

[0010] **Figure 5** illustrates an embodiment of a computer environment.

DETAILED DESCRIPTION

[0011] A method and apparatus are described for session key exchange.

[0012] Before describing an exemplary environment in which various embodiments of the present invention may be implemented, some terms that will be used throughout this application will briefly be defined:

[0013] As used herein, "Trusted Platform Module" or "TPM" means a device or function for use in providing secure operations. A TPM may comprises a set of functions and data that are common to all types of platforms, which must be trustworthy if the Subsystem is to be trustworthy; a logical definition in terms of protected capabilities and shielded locations. A TPM may contain platform configuration registers (PCRs), which store measurements of host system components that can be transmitted to another system in a trustworthy manner.

[0014] As used herein "public/private key pair" or "key pair" means a set of cryptographic keys used for public-key cryptography. The key pair consists of a "public key" and a "private key". The key pair may be used for encryption, in which case the public key is used for encrypting a message, and the private key used for decrypting the message. The key pair may also be used for digital signatures, in which case the private key is used for signing a message and the public key is used for verifying the message.

[0015] As used herein, a "public key" is the public half of a key pair. Among other uses, a public key may be used to encrypt a message to ensure that the message may only be decrypted by an entity holding the corresponding private key.

[0016] As used herein, a "private key" is the private or secret half of a key pair. Among other uses, a private key may be used to decrypt a message that has been encrypted with the corresponding public key.

[0017] As used herein, "session key" means a key to allow operation of a session for a system. A session key may be a randomly-generated key that is used for a single session, with a new session key provided for each session.

[0018] As used herein, "service key" means a key pair generated by a client, where the private key is stored on the client and the public key is stored by a service provider for use in connection with provision of service to a client. Service key includes a key pair used for encryption.

[0019] As used herein, "direct proof" or "direct proof protocol" means a process in which a first party and a second party establish trust by direct interaction between the parties. Direct proof includes a process in which trust is established without the use of a trusted third party.

[0020] As used herein, "platform" means an entity, including a computer, that transfers information to and from a user. As used herein, "configuration" means a manner in which a platform is set up. The terms includes a platform or a configuration as the terms are used in specifications of the TCG (Trusted Computing Group), including TCG Trusted Platform Module (TPM) specification, version 1.2, November 5, 2003; the TCG Main Specification, version 1.1b, 2003; the TCG Software Stack (TSS) Specification, Version 1.1, August 20, 2003; and the TCG PC Specific Implementation Specification, Version 1.1, August 18, 2003.

[0021] According to an embodiment of the invention, the provision of a service to a unit may be limited to a particular environment. In one embodiment, a process is described to securely exchange a session key between a platform and a challenger so that the challenger is assured that the session key is used only in a specific environment on a specific platform.

[0022] References are made herein to the Trusted Computing Group (TCG), which is an organization formed from the Trusted Computing Platform Alliance (TCPA). In addition to TCG applications, an embodiment of this invention also applies to any technologies or specifications derived from TCPA and to other security protocols. Specifications issued by the Trusted Computing Group involving secure operations include the TCG Trusted Platform Module (TPM) specification, version 1.2, November 5, 2003; the TCG Main Specification, version 1.1b, 2003; the TCG Software Stack (TSS) Specification, Version 1.1, August 20, 2003; and the TCG PC Specific Implementation Specification, Version 1.1, August 18, 2003.

[0023] According to an embodiment of the invention, software writing to a TCG-enabled platform, LaGrande Technology (LT) enabled platform, or similar technology is able to utilize a protocol to establish session keys for a platform. There are various established methods for exchanging session keys for a platform. However, an embodiment of the invention provides assurance that a session not only is limited to particular platform, but also to a specific configuration or configurations of the platform. Under an embodiment of the invention, even after a session key exchange is performed, the session key is not exposed unless this is done by the particular platform in a specified configuration.

[0024] **Figure 1** is an illustration of an embodiment of network operations. In this illustration, a client **105** includes a user **110**. The user may require a service to be provided by a service provider **120**. The service may comprise the utilization of any program, computer, or system. The client **105** and the service provider **120** may be connected through a network **125**, which may include the Internet. The client may include a trusted platform module (TPM) **115** for use in conducting secure transactions. The trusted platform module **115** includes a set of platform configuration registers (PCRs) **135** that contain values representing the platform's configuration. In certain embodiments, a trusted third party, such as a TCG defined privacy certification authority (CA) **130**, may be used to provide a credential, such as the issuance of an attestation identification key (AIK) certificate to the client. In other embodiments, no trusted third party is utilized. The AIK or other credential is used to establish mutual trust between the parties involved in the transaction. In this illustration, the service provider **120** requires sufficient assurance of the identification of the client and the specific limited use of the service before the service is provided. The service provider **120** may maintain policies, such as combinations of platform configuration register (PCR) values **140**, that describe allowable configurations for a client platform.

[0025] In one embodiment of the invention, trust is established between the first device and a second device using a trusted third party, such as a TCG defined privacy CA. In another embodiment, trust is established using a protocol between a first device and a second device with regard to a valid digital signature without the use of a trusted third party. In another embodiment, a trusted third party is used to establish trust, but a session key is provided without a challenger receiving information regarding which of multiple acceptable configurations is being utilized. Embodiments of the invention are not limited to the particular examples described herein. An embodiment of the invention can be applied in any circumstance in which a client requires a service from a provider and the provider requires assurance regarding the use of the service.

[0026] In a first embodiment of the invention, a user on a client may require a service from a service provider entity. The client selects a privacy CA that is known to be acceptable to the service provider. The client then generates a new AIK and obtains an AIK certificate from the privacy CA for use with the service provider. This process needs to be accomplished only once per service provider.

[0027] In this embodiment, the client requests an account with the service provider by sending the obtained AIK certificate to the service provider. The service provider requires a key, called a service key, on the client that can only be used when the client is in a particular configuration or in one of a set of particular configurations. The service provider has a policy that specifies what platform configurations are valid using a set of platform configuration register (PCR) values. The service provider provides the service key policy to the client and requests the client to generate a key pair with the specified set of PCR indexes and values and with specific attributes.

[0028] The client sends the request to the platform's trusted platform module (TPM). The TPM returns the public key component for the new service key, which the client returns to the service provider. The service provider at this point may not have sufficient data to trust the client to properly formulate a generate key request. However, the service provider may trust the TPM to properly report the attributes of the service key. The service provider requests the attributes of the service key using a CertifyKey function specifying the AIK sent in the original request from the client. The client sends the CertifyKey function to the TPM. The TPM computes a hash of the public component of the service key and its attributes, including the PCR indexes and values that gate or control the use of the service key. The TPM then uses the AIK to create a digital signature of the hash. The digital signature data is sent to the service provider.

[0029] The service provider validates the digital signature of the service key attributes and now may trust the TPM to restrict usage of the service key to the specified configuration or configurations. The service provider may now send any number of session keys in any number of sessions to the client using the service key. The service provider trusts that any session key will not be decrypted unless the client is in the configuration specified by the set of PCR attributes associates with the service key.

[0030] **Figure 2** is an illustration of transactions between a client **215** and a service provider **225** when the client **215** requests a service from the service provider **225**. The client **215** obtains an AIK certificate from a privacy CA **220**. The operation of the client is shown by the commands MakeIdentity/ActivateIdentity **230**. The privacy CA **220** provides the AIK certificate to the client **215**.

[0031] The client makes a request for service **240** and sends the AIK certificate **245** to the service provider **225**. The service provider **225** creates a new service key generation request **250**, the service key being limited to specific PCR values for certain allowable configurations. The service provider **225** sends to the client **215** the service key generation request to generate a key pair **255**. The client **215** then proceeds to generate the key pair **260** and returns the public key **265** to the service provider **225**. The service provider **225** proceeds to validate the public key **270,** including sending certify key request specifying the AIK **275** to the client **215**, which in turn sends the certify key request to the TPM **280**. The TPM generates a hash of the public key, associated PCR values, and relevant attributes as signed by the AIK, and the client returns the hash and digital signature data **285** to the service provider **225**. The service provider **225** validates the service key **290**, thereby enabling the issuance of a session key. The service provider **225** then may send a session key using the validated service key **295**, initiating the session, shown as the instruction Bind {session key} using the service key **298**.

[0032] For TCG operations, an encryption operation by an entity outside of a TPM is a "Bind" operation and a decryption operation within the TPM is an "Unbind" operation. The Bind operation is an encrypt operation of the session key using the public portion of the service key. Under an embodiment of the invention, the private portion of the service key cannot be used to decrypt (unbind) the session unless the platform's configuration (as represented by the appropriate set of PCRs) matches the restrictions placed on the usage of the key. This restriction is attested to by the CertifyKey operation. The service provider has confidence in the protection of the session key because it has verified that, even though the client has the private key that can decrypt the session key, the TPM will not do so unless the platform's configuration matches the configuration attested to by the CertifyKey for the service key.

[0033] Under an embodiment of the invention, the processes described above and illustrated in Figure 2, as well as the processes illustrated in Figures 3 and 4, can be combined without affecting the general operation of the system. For example, the generation of the key pair, returning of the public key and returning of certifying information (the hash of the public key, PCR information, and attributes, signed by the AIK) may be accomplished in a single process with a single result.

[0034] In the embodiments shown in Figure 2, Figure 3, and Figure 4, the horizontal dashed lines delineate phases of a registration and use process. Components and actions illustrated above the upper dashed line (**205**, **305**, and **405**) are performed once per account setup with a particular service provider. Components and actions between the upper dashed line and the lower dashed line (**210**, **310**, and **410**) are generally accomplished once per account setup with a particular service provider, but may be repeated if necessary to reset keys (such as with a forgotten password) or, for example, for the establishment of secondary accounts under a master account. Components and actions illustrated below the lower dashed line are to be done each time a new session is needed.

[0035] In an embodiment of the invention, the establishment and proof of a key's validity is not required to be accomplished in a protected or validated environment. However, a service provider may desire to have this additional validation. Therefore, the AIK can be used (either as a separate process or combined with other processes) to prove the current state of the platform. This may be done while performing the operation either by using an AIK with a set of PCR restrictions or by performing a TCG Quote function.

[0036] According to a second embodiment of the invention, a session key exchange is performed using a method for establishing trust between a first device and a second device with regard to a valid signature without revealing identity. The method may include a direct proof protocol. In the embodiment described above, a client and a service provider agree on a Privacy CA, which may be difficult in certain circumstances.

In addition, the user on the client may not want to expose the client-specific information required to establish an AIK. A direct proof protocol provides an alternative mechanism.

[0037] **Figure 3** is an illustration of a direct proof protocol embodiment. In Figure 3, there is a transaction between a client **315** and a service provider **320**, the client **315** requesting a service from the service provider **320**. The client **315** engages direct proof functions **325** with the direct proof engine **335** of the service provider. Using the direct proof protocol **330**, the service provider obtains an AIK for the client **340**.

[0038] The client then makes a request for service **345** to the service provider **320**. The service provider **320** creates a new service key generation request **348**, the service key being limited to specific PCR values for certain allowable configurations. The service provider **320** sends to the client **315** the service key generation requests to generate a key pair **350**. The client **315** then proceeds to generate the key pair **355** and returns the public key **360** to the service provider **320**. The service provider **320** proceeds to validate the public key **365**, including sending a certify key request specifying the AIK **370** to the client **315**, which in turn sends the certify key request to the TPM **375**. The TPM generates a hash of the public key, associated PCR values, and relevant attributes as signed by the AIK, and the client returns the hash and digital signature data **380** to the service provider **320**. The service provider **320** validates the service key **385**, thereby enabling the issuance of a session key. The service provider **320** then may send a session key using the validated service key **390**, initiating the session, shown as the instruction Bind {session key} using the service key **395**.

[0039] The first embodiment of the invention illustrated above, which utilizes a privacy CA, provides that the service provider knows the set of PCRs that are valid for a client. The provision of this information may present a privacy violation or problem because these values may be specific to one platform or a small set of individual platforms, thereby potentially identifying the platform.

[0040] According to a third embodiment of the invention, a Yes/No attestation protocol is used. The use of such a protocol allows the service provider to send certain acceptable PCR value sets to the client, which in turn sends the PCR value sets to the TPM. The service provider trusts the TPM to check the attributes of the key against the set of acceptable values sets and confirm or refute that there is at least one match with the platform. The embodiment of the invention allows a service provider to send a session key to a known, authorized and valid platform in a trusted configuration, but without identifying the particular configuration in use.

[0041] **Figure 4** illustrates a secure transaction utilizing a yes/no attestation protocol. In this illustration, transactions occur between a client **415** and a service provider **425** when the client **415** requests a service from the service provider **425**. The client **415** obtains an AIK certificate from a privacy CA **420**. The operation of the client is shown by the commands MakeIdentity/ActivateIdentity **430**. The privacy CA **420** provides the AIK certificate to the client **415**.

[0042] The client makes a request for service **440** and sends the AIK certificate **445** to the service provider **425**. The service provider **425** creates a new service key generation request **450**, the service key being limited to specific PCR values for certain allowable configurations. The service provider **425** sends to the client **415** the service key generation request to generate a key pair **455**. The client **415** then proceeds to generate the key pair **460** and returns the public key **465** to the service provider **425**. The service provider **425** proceeds to validate the public key **470**. In this embodiment, the service provider sends a list of acceptable PCR value sets **475** to the client **415**, which in turn sends the data to the TPM **480**. The TPM certifies whether or not the list includes the particular configuration for the user by creating a digital signature with the AIK, and confirmation or refutation is sent **485** to the service provider **425**. In this manner, the service provider **425** receives assurance that the platform is in an acceptable configuration, without the client **415** providing more information than is required. The service provider **425** validates the service key **490**, thereby enabling the issuance of a session key. The service provider **425** then may send a session key using the validated service key **495**, initiating the session, shown as the instruction Bind {session key} using the service key **498**.

[0043] Techniques described here may be used in many different environments. **Figure 5** is block diagram of an exemplary environment. Under an embodiment of the invention, a computer **500** comprises a bus **505** or other communication means for communicating information, and a processing means such as one or more processors **510** (shown as **511** through **512**) coupled with the first bus **505** for processing information.

[0044] According to an embodiment of the invention, the computer **500** includes a trusted platform module (TPM) **555**. The trusted platform module is used in secure transactions, such as transactions in which the computer **500** requests a service from a service provider.

[0045] The computer **500** further comprises a random access memory (RAM) or other dynamic storage device as a main memory **515** for storing information and instructions to be executed by the processors **510**. Main memory **515** also may be used for storing temporary variables or other intermediate information during execution of instructions by the processors **510**. The computer **500** also may comprise a read only memory (ROM) **520** and/or other static storage device for storing static information and instructions for the processor **510**.

[0046] A data storage device **525** may also be coupled to the bus **505** of the computer **500** for storing information and instructions. The data storage device **525** may include a magnetic disk or optical disc and its corresponding drive, flash memory or other nonvolatile memory, or other memory device. Such elements may be combined together or may be separate components, and utilize parts of other elements of the computer **500**.

[0047] The computer **500** may also be coupled via the bus **505** to a display device **530**, such as a liquid crystal display (LCD) or other display technology, for displaying information to an end user. In some environments, the display device may be a touch-screen that is also utilized as at least a part of an input device. In some environments, display device **530** may be or may include an auditory device, such as a speaker for providing auditory information. An input device **540** may be coupled to the bus **505** for communicating information and/or command selections to the processor **510**. In various implementations, input device **540** may be a keyboard, a keypad, a touch-screen and stylus, a voice-activated system, or other input device, or combinations of such devices. Another type of user input device that may be included is a cursor control device **545**, such as a mouse, a trackball, or cursor direction keys for communicating direction information and command selections to processor **510** and for controlling cursor movement on display device **530**.

[0048] A communication device **550** may also be coupled to the bus **505**. Depending upon the particular implementation, the communication device **550** may include a transceiver, a wireless modem, a network interface card, or other interface device. The computer **500** may be linked to a network or to other devices using the communication device **550**, which may include links to the Internet, a local area network, or another environment. In an embodiment of the invention, the communication device **550** may provide a link to a service provider over a network.

[0049] In the description above, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without some of these specific details. In other instances, well-known structures and devices are shown in block diagram form.

[0050] The present invention may include various processes. The processes of the present invention may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor or logic circuits programmed with the instructions to perform the processes. Alternatively, the processes may be performed by a combination of hardware and software.

[0051] Portions of the present invention may be provided as a computer program product, which may include a machine-readable medium having stored thereon instructions, which may be used to program a computer (or other electronic devices) to perform a process according to the present invention. The machine-readable medium may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs (compact disk read-only memory), and magneto-optical disks, ROMs (read-only memory), RAMs (random access memory), EPROMs (erasable programmable read-only memory), EEPROMs (electrically-erasable programmable read-only memory), magnet or optical cards, flash memory, or other type of media / machine-readable medium suitable for storing electronic instructions. Moreover, the present invention may also be downloaded as a computer program product, wherein the program may be transferred from a remote computer to a requesting computer by way of data signals embodied in a carrier wave or other propagation medium via a communication link (e.g., a modem or network connection).

[0052] Many of the methods are described in their most basic form, but processes can be added to or deleted from any of the methods and information can be added or subtracted from any of the described messages without departing from the basic scope of the present invention. It will be apparent to those skilled in the art that many further modifications and adaptations can be made. The particular embodiments are not provided to limit the invention but to illustrate it. The scope of the present invention is not to be determined by the specific examples provided above but only by the claims below.

[0053] It should also be appreciated that reference throughout this specification to "one embodiment" or "an embodiment" means that a particular feature may be included in the practice of the invention. Similarly, it should be appreciated that in the foregoing description of exemplary embodiments of the invention, various features of the invention are sometimes grouped together in a single embodiment, figure, or description thereof for the purpose of streamlining the disclosure and aiding in the understanding of one or more of the various inventive aspects. This method of disclosure, however, is not to be interpreted as reflecting an intention that the claimed invention requires more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed embodiment. Thus, the claims are hereby expressly incorporated into this description, with each claim standing on its own as a separate embodiment of this invention.